UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(i) 600 Broadway, Apt. 34D, Menands, NY; (ii) Jonathan Macdonald; and (iii) Certain Electronic Media

Case No. 1:25-sw-106 (DJS)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Receipt and possession of child pornography

The application is based on these facts:

See Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Dominick Canty
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: May 13, 2025

Judge's signature

City and state: Albany, New York

Magistrate Judge Daniel J. Stewart
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

(i) IN THE MATTER OF THE SEARCH OF 600 BROADWAY, APT. 34D, MENANDS, NY; (ii) JONATHAN MACDONALD; AND (iii) CERTAIN ELECTRONIC MEDIA	Case No. 1:25-sw-106 (DJS)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Dominick Canty, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since September 2019. I am assigned to the Albany Field Office and specifically to a squad investigating federal violations concerning child pornography and the sexual exploitation of children. I have gained experience investigating such crimes through training in seminars, classes, and everyday work related to conducting these types of investigations. Previously I was assigned to an Internet Crimes Against Children squad in FBI Los Angeles, where I have experience investigating subjects who have exploited children, typically by sending child sexual abuse material over the internet. Prior to being employed by the FBI as a Special Agent, I was employed by the FBI as an Intelligence Analyst for approximately two years, where I had experience performing analysis for investigations involving drug trafficking and transnational organized crime.

2. I have also received formal training regarding crimes against children and I have also consulted with other members of the FBI, who have training and experience in investigating child exploitation offenses involving the possession, distribution, production, and receipt of child pornography.

3. The facts in this affidavit come from my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. This affidavit is made in support of an application for a federal search warrant to search (A) the residence located at 600 Broadway, Apt 34D, Menands, NY 12204 ("SUBJECT PREMISES"), to include any garage, whether attached or unattached, and any outbuildings on the property under the dominion and control of the resident or occupant of the SUBJECT PREMISES, (B) the person of JONATHAN MACDONALD, and (C) any computers, computer equipment, and/or any other electronic media located during the execution of the search warrant. Located within the places and items to be searched, I seek to seize evidence, fruits, and instrumentalities of criminal violations relating to the knowing receipt and possession of child pornography, as more particularly described in Attachment B.

5. The SUBJECT PREMISES, further described in Attachment A, is in a multi-unit dwelling consisting of apartments A, B, C and D. The complex is a brick structure with green shutters and a yellow door with the marking "34." Contained in the complex is the SUBJECT PREMISES itself, apartment "D."

6. The statements contained in this affidavit are based on my involvement in this investigation, as well as information provided to me by other law enforcement officers involved in this investigation, and upon my training and experience. Because this affidavit is being submitted for the limited purpose of seeking a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are

necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252A(a)(2)(A) (Receipt of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography) exists at the SUBJECT PREMISES, on the person of JONATHAN MACDONALD, and on computers and electronic media found in the course of the search.

COMPUTERS AND CHILD PORNOGRAPHY

7. The use of computers has significantly reduced the amount of resources needed to produce, communicate, distribute, and share child pornography. For example, child pornographers can transfer photographs into a computer readable format with a scanner, and images captured on a digital camera can be transferred directly onto a computer. Photos taken on a digital camera are also stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store over 8000 high resolution photographs. Digital video camcorders can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer. Modems allow computers to connect to one another through the use of a telephone, cable, or wireless internet connection. Cellular telephones are often equipped with photo and video capabilities, which allow an individual to digitally shoot, store, send, and/or receive child pornography all with one device. Additionally, cellular telephones are themselves a means of communication when used to send text and electronic mail messages. Electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography: a computer drive can store hundreds of thousands of

images at very high resolution.

9. The internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography. Services offered by internet portals such as Yahoo!, Hotmail, and Gmail (among others) allow a user to set up an account with a remote computing service, which provides email as well as electronic storage for computer files in a variety of formats. Therefore, a user can set up an online storage account from any computer that has access to the internet. Evidence that the computer has been used to facilitate online storage of child pornography may be found on the computer.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (e.g., a user can save an e-mail as a file on the computer or save the location of his or her favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally (e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or Internet Service Provider (ISP) client software, among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a computer also creates logs, indices, and registries indicating when a computer was used, which user was logged on, and when data was accessed, shared, transferred, or downloaded. A forensic examiner can often recover evidence which shows when a computer was sharing files, and even some of the files that were uploaded or downloaded. Such

information may be maintained indefinitely until overwritten by other data. Cellular telephones also allow the user to save or store text messages and e-mail messages received by the phone for later viewing or distributing, and, even if deleted, a forensic examiner can often recover evidence of these messages.

12. The internet can be accessed from a computer network or ISP that connects to the internet. The ISP assigns each user an internet protocol (IP) address. Each IP address is unique. Every computer or device on the internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255 (e.g., 74.76.48.210). Each time a user accesses the internet, the computer from which that user initiates access is assigned an IP address. A central authority provides each ISP with a limited block of IP addresses for use by that ISP's user(s) or subscriber(s). Most ISPs employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an internet session each time a customer or subscriber accesses the internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses may also be static, which means that an ISP assigns a user's computer a particular IP address for use each time that computer accesses the internet. The ISP may log the date, time, and duration of the internet session for each IP address and can identify the user of that IP address for any session from these records, depending on the ISP's record retention policies.

13. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when files have

been deleted, they may be recoverable months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. In addition, a computer's operating system may keep a record of deleted data in what is known as a "swap" or "recovery" file. Similarly, files that have been viewed via the internet are automatically downloaded into a temporary internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

THE INVESTIGATION AND FACTUAL BASIS

14. I have reviewed two depositions taken by the Saratoga County Sheriff's Office. The first deposition was given by a Target Employee ("Employee 1") who is a supervisor for the Loss Prevention Department at the Target warehouse in Wilton, NY. According to the deposition:

a. At approximately 9:00AM on April 13th, 2025, a USB-A adaptor containing a Micro SD card was found in the men's bathroom by a Target employee. The Micro SD card was turned over to the floor supervisor and left in the Lost and Found for a couple of weeks.

b. A couple days later, during a monthly purge of Lost and Found items, a different Target Employee ("Employee 2") who also works in the Lost and Found made a

copy of the Micro SD card and reviewed it. Employee 2 identified child pornography on the Micro SD card and reported it to Employee 1.

c. Employee 2 claimed that the Micro SD card belongs to MACDONALD based on seeing Instagram information on the MicroSD card indicating it belongs to MACDONALD, as explained further below.

15. I have reviewed a second deposition taken by the Saratoga County Sheriff's Office. The deposition was given by a Target Employee ("Employee 2") whose responsibilities are purging lost and found items located in the store. According to this deposition:

a. On April 26, 2025, Employee 2 began purging the Lost and Found items and identified the Micro SD card. In an effort to identify the owner, Employee 2 made a copy of the Micro SD card. On the Micro SD card, Employee 2 identified files containing child pornography and reported it to Employee 1.

b. Employee 2 identified screenshots of an Instagram account on the Micro SD card. These screenshots contained photos of young women. In the bottom right corner of the screen, there was an Instagram profile picture of a cat with its eyes closed lying on a blue blanket or towel. This profile picture showed what account was logged into Instagram at that time. Based on his knowledge of this profile picture, Employee 2 identified MACDONALD as the account holder of the Instagram account that was logged in.

c. After reviewing the copy, Employee 2 destroyed the copy he had made of the content on the Micro SD card. The original Micro SD card remained in the lost and found at the Target Warehouse.

16. On April 28, 2025, the Micro SD card was turned over, in a sealed bag, to Deputy Kitts of the Saratoga County Sheriff's Office by Employee 1. The Micro SD card was inserted into a USB-A adaptor allowing it to be read on digital devices such as desktop computers, laptops and tablets. On May 6, 2025, I reviewed the content on the Micro SD card utilizing a write blocker, which prevented the USB-A adaptor and Micro SD card from being modified in this process, and identified multiple images and videos of child pornography present on the device, including a video that was approximately 27 minutes and 18 seconds long containing clips of various child pornography. The video depicted the following:

a. At approximately 32 seconds in the video, there appears a prepubescent female, 8-10 years of age and naked, sitting on her rear. For approximately 1 minute and 30 seconds in the video the female is spreading her legs inserting her finger into her vagina.

b. At approximately 19 minutes and 40 seconds in the video is an image of a prepubescent female, approximately 4-6 years of age, unclothed from the waist down and lying on her back. In the image is an adult male penis hovering over the vaginal area of the prepubescent female. On the stomach of the prepubescent female is a clear substance similar to semen.

17. Based on my training and experience and the images/videos I reviewed I believe the images and videos on the Micro SD card are images and videos that were screenshotted and recorded utilizing a mobile device such as a cell phone. Additionally, I identified folders on the Micro SD card that suggests that the mobile application XRecorder was used to create images and videos. XRecorder which is an application that can be used to record screens of mobile

devices.

18. Numerous Instagram screenshots with a visible profile photograph or other identifier in the screen shot were also located on the SD card, and, as further described below, identify the owner to be MACDONALD.

IDENTIFICATION OF MACDONALD AS THE OWNER

19. The Saratoga County Sheriff's Office conducted a reverse image search of the Instagram screenshots located on the Micro SD card. Through open-source searches, the Instagram profile "waduhek6193" was identified as containing the exact same profile picture as the Instagram Profile picture located on the Micro SD card.

20. On May 8, 2025, pursuant to an administrative subpoena for records associated with Instagram account "waduhek6193", the subscriber was identified as MACDONALD.

21. According to the deposition given by Employee 1, MACDONALD was seen on Target Security cameras entering the bathroom where the Micro SD card was found at approximately 12:00AM on April 13, 2025. This was about 9 hours before the Micro SD card was found by a Target employee and submitted to Lost and Found.

22. Based on information provided by Employee 1, MACDONALD is a worker formerly employed at the Target warehouse in Wilton, NY where the Micro SD card was found.

PRIOR INVESTIGATION INVOLVING MACDONALD

23. In December 2020, the National Center for Missing and Exploited Children generated a CyberTip after it was reported that known child pornography had been uploaded to a Google Drive account associated with the email address mesohorny16@gmail.com. Based on the CyberTip, New York State Police identified MACDONALD as a suspect, and conducted a

knock and talk at the location where he was living at the time. MACDONALD admitted that the email address associated with the CyberTip was his, but claimed the account had been hacked approximately one year before. A manual preview of a phone provided to NYSP by MACDONALD during the knock and talk was conducted on site with MACDONALD's consent. The manual preview of the device was negative for child pornography, and it was returned to MACDONALD. No digital forensic examination of the phone wase conducted, and there was no search of the residence for other devices that could have been the source of the CyberTipline Report, or that could have contained child pornography, and the investigation was closed.

IDENTIFICATION OF MACDONALD RESIDENCE

24. On May 8, a NYS DMV query was conducted and a 2014 Ford Escape NY plate KDM-6782 was found to be registered to MACDONALD. On May 8, 2025, FBI TFO Michelle Crandall identified the vehicle parked in front of 600 Broadway, Building 34, Menands, NY.

25. A query of Accurint was conducted and MACDONALD was found to have an address of 600 Broadway, Apt 34D, Menands, NY.

CHARACTERISTICS OF CHILD PORNOGRAPHY USERS

26. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and attempt to receive child pornography:

i. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from

fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

ii. Those that receive and attempt to receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

iii. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

iv. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence or vehicle, to enable the collector to view the collection, which is valued

highly.

v. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

vi. Those that receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

27. It is reasonable to believe that some or all of the records sought to be seized will be in electronic/digital format. Searching and seizing information from computer systems and other storage media (including PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic examiner in a laboratory or other controlled environment. This is true for the reasons set out below.

28. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in desktop computers are capable of storing millions of pages of text; the storage capacity of other electronic devices

(e.g. a micro drive, a thumb drive, etc.) can also be significant. For instance, a single 1 gigabyte of storage media is the electronic equivalent of approximately 500,000 pages of double spaced text. Most computer and electronic devices have capacities well in excess of a single gigabyte.

29. The search through the computer (or other electronic media) itself is a time-consuming process. Software and individual files can be password-protected. Files can be placed in hidden directories; files can be mislabeled or be labeled with names that are misleading. Similarly, files that contain innocent appearing names (e.g., "Smith.ltr") can in fact be electronic commands to electronically cause the data to self-destruct. Also, files can be deleted, but, unlike documents that are destroyed, the information and data from deleted electronic files usually remains on the storage device until it is overwritten by the computer. For example, the computer hard drive stores information in a series of "sectors," each of which contains a limited number of electronic bytes, usually 512. These sectors are generally grouped to form clusters. There are thousands or millions of such clusters on a hard drive. A file's clusters might be scattered throughout the drive (for example, part of a memo could be at Cluster 163, while the next part of the memo might be stored at Cluster 2053). For a non-deleted file, there are "pointers" that guide the computer in piecing the clusters together. For a file that has been deleted, the pointers have been removed. Therefore, the forensic examination would include the piecing together of the associated clusters that made up the deleted file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time-consuming procedure to review the contents of the computer storage device so as to insure the integrity of the data and/or evidence. A single computer and related equipment could take many days to analyze properly.

30. Computer storage media are used to save copies of files and communications, and

printers are used to make paper copies of these communications and files. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. All these parts of a computer are integrated into the entire operation of a computer. In order to evaluate the evidence most effectively, the computers and all of the related computer equipment described above should be available to a computer investigator/analyst.

31. Therefore, based upon my knowledge, training, and experience, as well as information related to me by others involved in forensic examination of computers, I am aware that searches for and seizures of evidence from computers commonly require agents to seize most or all of a computer system's input/output and peripheral devices (including other storage media), in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. In order to fully retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit.

32. Furthermore, searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

33. Further, computers, hard drives, removable media and other electronic devices have the capacity to retain information, even after that information has been deleted by the user. Thus, images, videos and other files associated with the receipt, distribution and possession of child pornography may be recovered from electronic and digital media, even if those files were previously deleted.

34. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively named, erased, compressed, encrypted, or password protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

35. A number of computer storage devices are quite small and portable, and can be easily hidden on a person. For instance, digital cameras can store numerous digital images on a disk approximately the size of a postage stamp. In addition, thumb drives can hold numerous images and computer videos.

Biometric Access to Devices

36. The requested warrant would also permit law enforcement to compel Jonathan MACDONALD to unlock any devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. Many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include

fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft

devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. Users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. The passcodes or passwords that would unlock MACDONALD'S devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not

been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

37. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the requested warrant would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of MACDONALD to the fingerprint scanner of the devices found at the SUBJECT PREMISES; (2) hold the devices found at the SUBJECT PREMISES in front of the face of MACDONALD and activate the facial recognition feature; and/or (3) hold the devices found at the SUBJECT PREMISES in front of the face of MACDONALD and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to require that MACDONALD state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to require MACDONALD to identify the

specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

Search Methodology to be Employed

38. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

i. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;

ii. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

iii. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

iv. surveying various file directories and the individual files they contain;

v. opening files in order to determine their contents;

vi. scanning storage areas;

vii. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

viii. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

LAW ENFORCEMENT AGENCIES ASSISTING FBI

39. This search warrant will be executed by your affiant and other FBI Special Agents. However, law enforcement officers from other agencies, to include the New York State Police (NYSP), Colonie Police Department, Rotterdam Police Department, the Saratoga County Sheriff's Office and Cohoes Police Department may be utilized by the FBI in the execution of this search warrant, to include the forensic examination of any electronic storage media devices that may be seized and later analyzed at a either an FBI or NYSP computer forensic laboratory.

Respectfully submitted,

Dominick Canty
Special Agent
Federal Bureau of Investigation

Attested to by the affiant in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure, this 13 day of May, 2025.

Hon. Daniel J. Stewart
United States Magistrate Judge

ATTACHMENT A

PLACES, PERSONS AND ITEMS TO BE SEARCHED

The places and items to be searched are: (A) the residence located at 600 Broadway Apt 34D, Menands, NY ("SUBJECT PREMISES"), to include any garage, whether attached or unattached, and any outbuildings on the property under the dominion and control of the resident or occupant of the SUBJECT PREMISES, (B) the person of JONATHAN MACDONALD, and (C) any computers, computer equipment, and/or any other electronic media located during the execution of the search warrant. Located within the places and items to be searched, I seek to seize evidence, fruits, and instrumentalities of criminal violations relating to the knowing receipt and possession of child pornography, as more particularly described in Attachment B.

600 Broadway Apt 34D, Menands, NY, depicted below, is a multi-unit dwelling consisting of apartments A, B, C and D. The complex is a brick structure with green shutters and a yellow door with the marking "34." Contained in the complex is apartment "D."

ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of Title 18, United States Code, Section 2252A (receiving or possessing child pornography).

Computers and Electronic Media

1. The authorization includes the search of electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with the affidavit submitted in support of this warrant.

2. Computer and electronic hardware, meaning any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. Included within the definition of computer and electronic hardware is any data processing hardware (such as central processing units and self-contained laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives, secure digital (SD) cards, and diskettes, tape drives and tapes, optical and compact disk storage devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); digital cameras; related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); and any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).

3. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

4. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

5. Computer passwords and data security devices, meaning any devices, programs, or data—whether themselves in the nature of hardware or software—that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, data security hardware (such as encryption devices, chips, and circuit boards); passwords; data security software or information (such as test keys and

encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.

6. Any computer or electronic records, documents, and materials referencing relating to the above-described offenses. Such records, documents, or materials, as well as their drafts or modifications, may have been created or stored in various formats, including, but not limited to, any hand-made form (such as writing or marking with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negative, video tapes, motion pictures, or photocopies); any mechanical form (such as photographic records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact disks); or any information on any electronic or magnetic storage device (such as floppy diskettes, hard disks, CD-ROMs, optical disks, printer buffers, sort cards, memory calculators, electronic dialers, or electronic notebooks), as well as printouts or readouts from any magnetic storage device.

7. Any electronic information or data, stored in any form, which has been used or prepared for use either for periodic or random backup (whether deliberate, inadvertent, or automatically or manually initiated), of any computer or computer system. The form that such information might take includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, CD-ROM disks, video cassettes, and other media capable of storing magnetic or optical coding.

8. Any electronic storage device capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and using electronic data used to conduct computer or internet-based communications, or which contains material or data obtained through computer or internet-based communications, including data in the form of electronic records, documents, and materials, including those used to facilitate interstate communications, including but not limited to telephone (including mobile telephone) and ISPs. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed disks, external hard disks, removable hard disk cartridges, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, laser disks, USB drives, secure digital (SD) cards, or other memory storage devices.

Documents, Computer, and Internet Records

9. Records of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes (however and wherever written, stored, or maintained), books, notes, and reference materials.

10. Records of address or identifying information for the target(s) of the investigation, and any usernames (a.k.a., "Nics"), user IDs, eIDs (electronic ID numbers), and passwords.

11. Documents and records, including, for example, receipts, banking records, bills, statements, telephone records, and other similar indicia of ownership indicating occupation, possession, or control over the residence and/or possession of the searched items located therein.

12. Computer records and evidence identifying who the particular user was who distributed, transmitted, downloaded or possessed any child pornography found on any computer or computer media (i.e. evidence of attribution).

Materials Relating to Child Pornography, Child Erotica, and Depictions of Minors

13. Any and all child pornography, and any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors, as those terms are defined in Title 18, United States Code, Section 2256.

14. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

15. Any and all notebooks and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

16. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes.

Photographs of Search

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

Biometric Access

18. During the execution of the search of the locations described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of JONATHAN MACDONALD upon a device; (2) hold a device found at the location in front of the face of JONATHAN MACDONALD and activate the facial recognition feature; and (3) hold a device found at the location before the eyes of JONATHAN MACDONALD and activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.